## ***LAB11:***

### Task0:

Am creat noii useri:

```
student in ~ at isc-vm …
→ sudo useradd -m -s /bin/bash red

student in ~ at isc-vm …
→ sudo useradd -m -s /bin/bash green

student in ~ at isc-vm …
→ sudo useradd -m -s /bin/bash blue

student in ~ at isc-vm …
```

Am copiat .ssh ul lui student in fiecare nou user:

```
student in ~ at isc-vm …
→ sudo cp -r /home/student/.ssh /home/red/

student in ~ at isc-vm …
→ sudo cp -r /home/student/.ssh /home/green/

student in ~ at isc-vm …
→ sudo cp -r /home/student/.ssh /home/blue/

student in ~ at isc-vm …
```

Am adaugat drepturi si ownership:

```
student in ~ at isc-vm …
→ sudo chown -R red:red /home/red/.ssh

student in ~ at isc-vm …
→ sudo chown -R green:green /home/green/.ssh

student in ~ at isc-vm …
→ sudo chown -R blue:blue /home/blue/.ssh

student in ~ at isc-vm …
→ sudo chmod 777 /home/red/.ssh

student in ~ at isc-vm …
→ sudo chmod 777 /home/green/.ssh

student in ~ at isc-vm …
→ sudo chmod 777 /home/blue/.ssh
```

## Task1:

Generez public key pentru toti userii:

```
red@isc-vm:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/red/.gnupg' created
gpg: keybox '/home/red/.gnupg/pubring.kbx' created
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: redVM
Email address: red@cs.pub
```

```
gpg: /home/red/.gnupg/trustdb.gpg: trustdb created
gpg: key B0FD14FC0064AB42 marked as ultimately trusted
gpg: directory '/home/red/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/red/.gnupg/openpgp-revocs.d/5D3E0B92F93DE1C14A464C9EB0FD14FC0064AB42.rev'
public and secret key created and signed.

pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      5D3E0B92F93DE1C14A464C9EB0FD14FC0064AB42
uid                      redVM <red@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]
```

```
green@isc-vm:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/green/.gnupg' created
gpg: keybox '/home/green/.gnupg/pubring.kbx' created
Note: Use "gpg --full-generate-key" for a full featured key generation dialo
g.

GnuPG needs to construct a user ID to identify your key.

Real name: greenVM
Email address: green@cs.pub
You selected this USER-ID:
    "greenVM <green@cs.pub>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit?
```

```
gpg: /home/green/.gnupg/trustdb.gpg: trustdb created
gpg: key C5455C54107F3153 marked as ultimately trusted
gpg: directory '/home/green/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/green/.gnupg/openpgp-revocs.d/FD64C9E9187B667C2DF65C59C5455C54107F3153.rev'
public and secret key created and signed.

pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      FD64C9E9187B667C2DF65C59C5455C54107F3153
uid                      greenVM <green@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]
```

```
blue@isc-vm:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/blue/.gnupg' created
gpg: keybox '/home/blue/.gnupg/pubring.kbx' created
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: blueVM
Email address: blue@cs.pub
You selected this USER-ID:
    "blueVM <blue@cs.pub>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit?
```

```
gpg: /home/blue/.gnupg/trustdb.gpg: trustdb created
gpg: key CB35943C0B78FDC8 marked as ultimately trusted
gpg: directory '/home/blue/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/blue/.gnupg/openpgp-revocs.d/038E1DAFDBBBA6081590E8C5CB35943C0B78FDC8.rev'
public and secret key created and signed.

pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      038E1DAFDBBBA6081590E8C5CB35943C0B78FDC8
uid                      blueVM <blue@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]
```

Importat cheia lui red in green:

```
red@isc-vm:~$ gpg --export --armor red@cs.pub > /home/red/red_pubkey.asc
red@isc-vm:~$ cp /home/red/red_pubkey.asc /tmp/red_pubkey.asc
red@isc-vm:~$ chmod 644 /tmp/red_pubkey.asc
red@isc-vm:~$ exit
logout

student in ~ at isc-vm took 1m 42.1s …
➜ sudo -u green -i
green@isc-vm:~$ gpg --import /tmp/red_pubkey.asc
gpg: key B0FD14FC0064AB42: public key "redVM <red@cs.pub>" imported
gpg: Total number processed: 1
gpg:               imported: 1
green@isc-vm:~$ gpg --list-keys
/home/green/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      FD64C9E9187B667C2DF65C59C5455C54107F3153
uid           [ultimate] greenVM <green@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]

pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      5D3E0B92F93DE1C14A464C9EB0FD14FC0064AB42
uid           [ unknown] redVM <red@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]

green@isc-vm:~$
```

Trimitere mesaj:

```
➜ sudo -u red -i
red@isc-vm:~$ echo "This is a secret message" > /home/red/secret_file.txt
```

```
red@isc-vm:~$ gpg --encrypt --recipient green@cs.pub /home/red/secret_file.txt
gpg: 1D6573E874FE4485: There is no assurance this key belongs to the named user

sub  rsa3072/1D6573E874FE4485 2024-05-23 greenVM <green@cs.pub>
 Primary key fingerprint: FD64 C9E9 187B 667C 2DF6  5C59 C545 5C54 107F 3153
      Subkey fingerprint: 670D 2DD1 0D44 E2EC 8225  E7A1 1D65 73E8 74FE 4485

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
red@isc-vm:~$ cp /home/red/secret_file.txt.gpg /tmp/
red@isc-vm:~$ chmod 644 /tmp/secret_file.txt.gpg
red@isc-vm:~$ exit
logout

student in ~ at isc-vm took 1m 11.9s …
➜ sudo -u green -i
green@isc-vm:~$ cp /tmp/secret_file.txt.gpg /home/green/
green@isc-vm:~$ gpg --decrypt /home/green/secret_file.txt.gpg > /home/green/decrypted_file.txt
gpg: encrypted with 3072-bit RSA key, ID 1D6573E874FE4485, created 2024-05-23
      "greenVM <green@cs.pub>"
green@isc-vm:~$ cat /home/green/decrypted_file.txt
This is a secret message
green@isc-vm:~$
```

Trust channel between ***blue*** and ***red*** using ***green:***

Green: Sign Red's Key and Export Both Keys:

```
green@isc-vm:~$ gpg --sign-key red@cs.pub.ro
gpg: key "red@cs.pub.ro" not found: No public key
green@isc-vm:~$ gpg --sign-key red@cs.pub

pub  rsa3072/B0FD14FC0064AB42
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: unknown       validity: unknown
sub  rsa3072/A025DBE38C9E2BBF
     created: 2024-05-23  expires: 2026-05-23  usage: E
[ unknown] (1). redVM <red@cs.pub>


pub  rsa3072/B0FD14FC0064AB42
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: 5D3E 0B92 F93D E1C1 4A46  4C9E B0FD 14FC 0064 AB42

     redVM <red@cs.pub>

This key is due to expire on 2026-05-23.
Are you sure that you want to sign this key with your
key "greenVM <green@cs.pub>" (C5455C54107F3153)

Really sign? (y/N) y
```

```
green@isc-vm:~$ gpg --export --armor green@cs.pub > /tmp/green_pubkey.asc
green@isc-vm:~$ gpg --export --armor red@cs.pub > /tmp/red_pubkey_signed.asc
green@isc-vm:~$ chmod 644 /tmp/green_pubkey.asc /tmp/red_pubkey_signed.asc
```

Blue: Import Both Keys and Sign Green's Key

```
blue@isc-vm:~$ cp /tmp/green_pubkey.asc /home/blue/
blue@isc-vm:~$ cp /tmp/red_pubkey_signed.asc /home/blue/
blue@isc-vm:~$ gpg --import /home/blue/green_pubkey.asc
gpg: key C5455C54107F3153: public key "greenVM <green@cs.pub>" imported
gpg: Total number processed: 1
gpg:               imported: 1
blue@isc-vm:~$ gpg --import /home/blue/red_pubkey_signed.asc
gpg: key B0FD14FC0064AB42: public key "redVM <red@cs.pub>" imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2026-05-23
```

```
blue@isc-vm:~$ gpg --sign-key green@cs.pub

pub  rsa3072/C5455C54107F3153
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: unknown       validity: unknown
sub  rsa3072/1D6573E874FE4485
     created: 2024-05-23  expires: 2026-05-23  usage: E
[ unknown] (1). greenVM <green@cs.pub>


pub  rsa3072/C5455C54107F3153
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: FD64 C9E9 187B 667C 2DF6  5C59 C545 5C54 107F 3153

     greenVM <green@cs.pub>

This key is due to expire on 2026-05-23.
Are you sure that you want to sign this key with your
key "blueVM <blue@cs.pub>" (CB35943C0B78FDC8)

Really sign? (y/N) y
```

```
blue@isc-vm:~$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   1  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2026-05-23
/home/blue/.gnupg/pubring.kbx
-----------------------------
pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      038E1DAFDBBBA6081590E8C5CB35943C0B78FDC8
uid           [ultimate] blueVM <blue@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]

pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      FD64C9E9187B667C2DF65C59C5455C54107F3153
uid           [  full  ] greenVM <green@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]

pub   rsa3072 2024-05-23 [SC] [expires: 2026-05-23]
      5D3E0B92F93DE1C14A464C9EB0FD14FC0064AB42
uid           [  undef ] redVM <red@cs.pub>
sub   rsa3072 2024-05-23 [E] [expires: 2026-05-23]
```

Pe userul red cream si semnam mesajul:

```
➜ sudo -u red -i
red@isc-vm:~$ echo "This is an important message" > /home/red/important_message.txt
red@isc-vm:~$ gpg --clearsign /home/red/important_message.txt
red@isc-vm:~$ cp /home/red/important_message.txt.asc /tmp/
red@isc-vm:~$ chmod 644 /tmp/important_message.txt.asc
red@isc-vm:~$ exit
logout
```

Verificam mesajul pe blue:

```
➜ sudo -u blue -i
blue@isc-vm:~$ cp /tmp/important_message.txt.asc /home/blue/
blue@isc-vm:~$ gpg --verify /home/blue/important_message.txt.asc
gpg: Signature made Thu 23 May 2024 04:45:32 PM EEST
gpg:                using RSA key 5D3E0B92F93DE1C14A464C9EB0FD14FC0064AB42
gpg: Good signature from "redVM <red@cs.pub>" [undefined]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 5D3E 0B92 F93D E1C1 4A46  4C9E B0FD 14FC 0064 AB42
blue@isc-vm:~$ exit
logout
```

Marcam cheia lui green Trusted si reverificam semnatura, am ales 5:

```
➜ sudo -u blue -i
blue@isc-vm:~$ gpg --edit-key green@cs.pub
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  rsa3072/C5455C54107F3153
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: unknown       validity: full
sub  rsa3072/1D6573E874FE4485
     created: 2024-05-23  expires: 2026-05-23  usage: E
[  full  ] (1). greenVM <green@cs.pub>

gpg> trust
pub  rsa3072/C5455C54107F3153
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: unknown       validity: full
sub  rsa3072/1D6573E874FE4485
     created: 2024-05-23  expires: 2026-05-23  usage: E
[  full  ] (1). greenVM <green@cs.pub>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
```

```
Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? (y/N) y

pub  rsa3072/C5455C54107F3153
     created: 2024-05-23  expires: 2026-05-23  usage: SC
     trust: ultimate      validity: full
sub  rsa3072/1D6573E874FE4485
     created: 2024-05-23  expires: 2026-05-23  usage: E
[  full  ] (1). greenVM <green@cs.pub>
Please note that the shown key validity is not necessarily correct
unless you restart the program.
```

Verificam din nou acum, si vedem ca apare Good signature:

```
blue@isc-vm:~$ gpg --verify /home/blue/important_message.txt.asc
gpg: Signature made Thu 23 May 2024 04:45:32 PM EEST
gpg:                using RSA key 5D3E0B92F93DE1C14A464C9EB0FD14FC0064AB42
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2026-05-23
gpg: Good signature from "redVM <red@cs.pub>" [full]
```

## TASK2:

Instalez utilitarul:

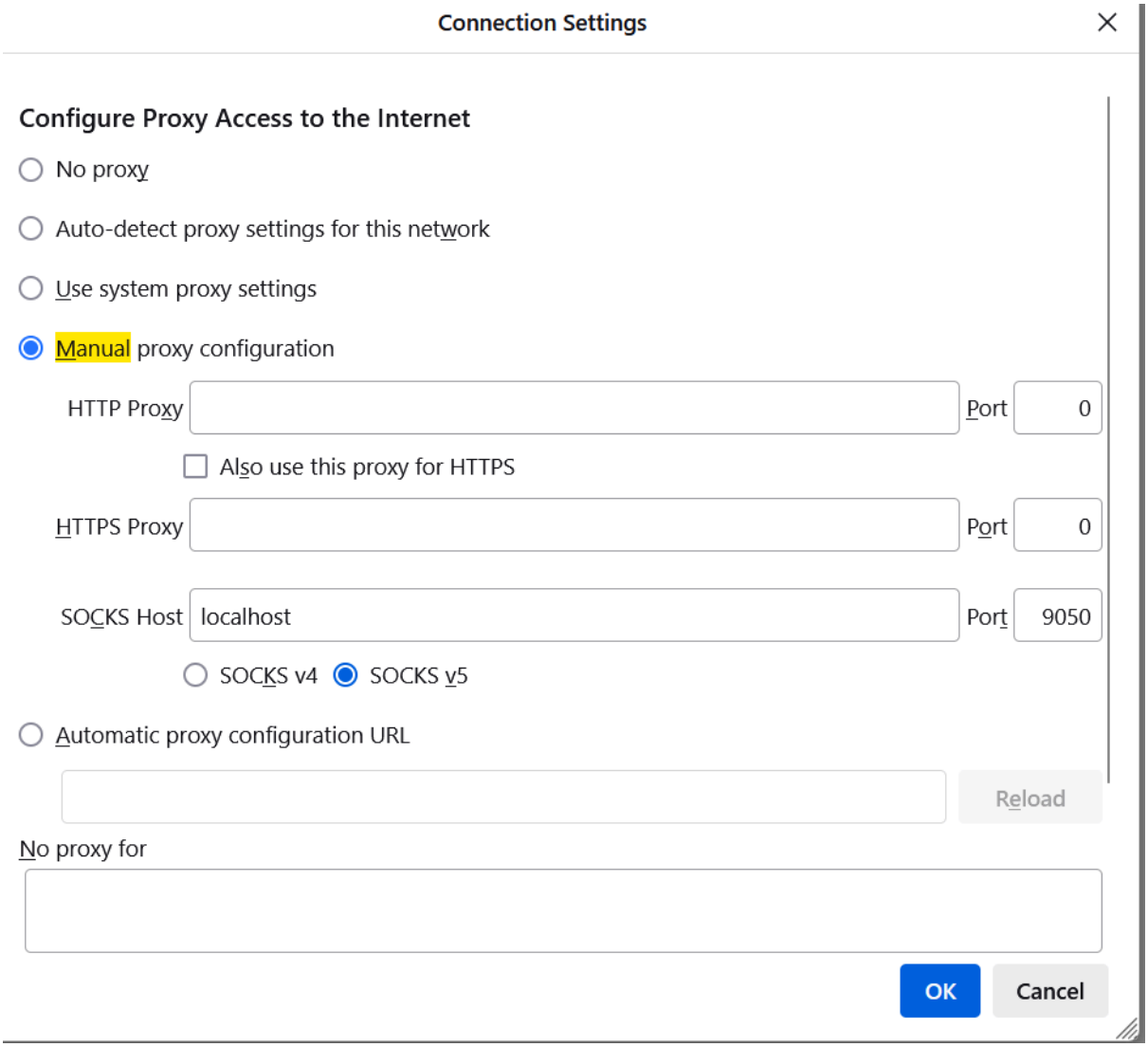
```
➜ sudo apt install tor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libmsgpackc2 libtermkey1 libtree-sitter0 libunibilium4 libvterm0 lua-luv
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher socat apparmor-utils nyx obfs4proxy
The following NEW packages will be installed:
```

Decomentez linia cu portul:

```
## Configuration file for a typical Tor user
## Last updated 9 October 2013 for Tor 0.2.5.2-alpha.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc

## Tor opens a socks proxy on port 9050 by default -- even if you don't
## configure one below. Set "SocksPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
SocksPort 9050 # Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.

## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SocksPolicy is set, we accept
## all (and only) requests that reach a SocksPort. Untrusted users who
## can access your SocksPort may be able to learn about the connections
## you make.
#SocksPolicy accept 192.168.0.0/16
#SocksPolicy reject *

## Logs go to stdout at level "notice" unless redirected by something
## else, like one of the below lines. You can have as many Log lines as
## you want.
##
## We advise using "notice" in most cases, since anything more verbose
## may provide sensitive information to an attacker who obtains the logs.
##
```

```
student in ~ at isc-vm …
➜ sudo systemctl restart tor

student in ~ at isc-vm …
➜ dig TXT +tcp +short o-o.myaddr.l.google.com @ns1.google.com | awk -F'"' '{ print $2}'
141.85.150.32

student in ~ at isc-vm …
➜ service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/lib/systemd/system/tor.service; enabled; vendor preset: enabled)
     Active: active (exited) since Thu 2024-05-23 16:52:39 EEST; 1min 29s ago
    Process: 23496 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 23496 (code=exited, status=0/SUCCESS)
        CPU: 1ms

May 23 16:52:39 isc-vm systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master)...
May 23 16:52:39 isc-vm systemd[1]: Finished Anonymizing overlay network for TCP (multi-instance-master).

student in ~ at isc-vm …
➜ torsocks --shell
New torified shell coming right up...

student in ~ at isc-vm …
➜ dig TXT +tcp +short o-o.myaddr.l.google.com @ns1.google.com | awk -F'"' '{ print $2}'
104.244.73.136

student in ~ at isc-vm …
➜
```

Am modificat in firefox:



Dupa conectare pe adresa: